Self-dual Codes over the Kleinian Four Group

Gerald Höhn

Mathematisches Institut der Universität Freiburg

Eckerstraße 1, 79104 Freiburg, Germany

E-mail: gerald@mathematik.uni-freiburg.de

Homepage: http://baby.mathematik.uni-freiburg.de/

26. Mai 2000

1 Introduction

In this work, we describe a new and natural fourth step in the series of analogies known to exist between binary codes, lattices and vertex operator algebras (see for example [CS93b, Höh95]).

Linear codes over the finite field $\mathbf{F}_4$ are studied in many papers (cf. [MOSW78, CPS79, Slo79, Slo78, LP90, CS90a, Huf90, Huf91]), but a developed theory for codes over the Kleinian four-group $K \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ is missing. It turns out that there is a similar rich theory as one has for binary linear codes. Parts of the results are known from some different viewpoints, but the use of Kleinian codes seems most natural.

We will prove all the results in terms of a theory for Kleinian codes, since this leads to a theory of its own right, although one can deduce most theorems from the corresponding results for self-dual vertex operator algebras or lattices or binary codes. To emphasize this relation, we will give after every theorem a list of references of the *analogue*[*] theorems for binary codes (B), lattices (L) and vertex operator algebras (V).

The second section contains the main definitions and first results. The next section describes the classification of odd and even self-dual codes up to length 8. In the fourth section, we study extremal codes. This are codes with the largest possible minimal weight. The fifth section is about designs for the space K^n. Section six deals with lexicographic constructions.

In the final section, we explain the relation and discuss some of the analogies with self-dual binary codes, lattices and vertex operator algebras in more detail. Self-dual Kleinian codes of length n can be identified with self-dual vertex operator superalgebras of rank $4n$ containing a vertex operator algebra of type $V_{D_4}^{\otimes n}$. From this viewpoint, Kleinian codes are a special case of codes over a 3-dimensional topological quantum field theory.

Our motivation behind the introduction of Kleinian codes was to have an additional testbed besides binary codes and lattices for the understanding of vertex algebras. Kleinian codes have already found applications as quantum codes and some of the results have been extended to and sharpened for codes of larger length.

---

[*] An additional asterisk indicates that the theorem can be obtained from the analogues theorems for binary codes, lattices or vertex operator algebras by the relations described in the final section.

2 Definitions and basic results

Denote the elements of the Kleinian four group $K \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ by 0, a, b and c, where 0 is the neutral element. The automorphism group of K is S_3, the permutation group of the three nonzero elements a, b and c. A *code* C over K of length n is a subset of the words of length n over the alphabet K, i.e. consists of vectors $\mathbf{x} = (x_1, \ldots, x_n)$, $x_i \in K$, the *codewords* of C. The *weight* $\mathrm{wt}(\mathbf{x})$ of a codeword $\mathbf{x}$ is the number of nonzero x_i. The *minimal weight* of C is defined by
$$d = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \ \mathbf{x} \neq 0\}.$$

The code C is called *linear* if C is a subgroup of the abelian group $K^n \cong \mathbf{Z}_2^{2n}$. A linear code has 4^k elements with $k \in \frac{1}{2}\mathbf{Z}$ and we denote k the *dimension* of the code. All codes in this article are assumed to be linear. A code of length n, dimension k and minimal weight d is shortly denoted as a $[n, k, d]$- or $[n, k]$-code. Let now C be a $[n, k]$-code.

An important part of the structure which makes the theory of Kleinian codes interesting is the *scalar product* $(.\,,\,.) : K^n \times K^n \longrightarrow \mathbf{F}_2$, $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} x_i \cdot y_i$, where the symmetric bilinear dot product $\cdot : K \times K \longrightarrow \mathbf{F}_2$ is defined by $a \cdot b = b \cdot a = 1$, $a \cdot c = c \cdot a = 1$, $b \cdot c = c \cdot b = 1$ and zero otherwise. The *dual code* $C^{\perp}$ is defined by

$$C^{\perp} = \{\mathbf{x} \in K^n \mid (\mathbf{x}, \mathbf{y}) = 0 \text{ for all } \mathbf{y} \in C\}$$

and has type $[n, n-k]$.

We call C *self-orthogonal* if $C \subset C^{\perp}$ and *self-dual* if $C^{\perp} = C$.

The direct sum $C \oplus D$ of a $[n, k]$-code C and a $[m, l]$-code D is the direct product subgroup of $K^n \oplus K^m$ and has type $[n + m, k + l]$. If C can be written in a nontrivial way as a direct sum, C is called *decomposable,* otherwise *indecomposable.* Obviously $(C \oplus D)^{\perp} = C^{\perp} \oplus D^{\perp}$. Every code C is after a renumbering of the positions a direct sum of indecomposable codes. The isomorphism classes of the components are uniquely determined up to permutation.

The *(Hamming) weight enumerator* of C is the degree n polynomial

$$W_C(u, v) = \sum_{i=0}^{n} A_i \, u^{n-i} v^i \qquad \text{with } A_i = \#\{\mathbf{x} \in C \mid \mathrm{wt}(\mathbf{x}) = i\}.$$

The *complete weight enumerator* is the polynomial

$$\mathrm{cwe}_C(p, q, r, s) = \sum_{i,j,k,l} A_{i,j,k,l} \, p^i q^j r^k s^l,$$

where $A_{i,j,k,l}$ is the number of code words in C containing at i, j, k resp. l of the n positions the element 0, a, b resp. c. There is the obvious relation $W_C(u, v) = \mathrm{cwe}_C(u, v, v, v)$. Finally define for a natural number g the *poly-* or *g-weight enumerator* W_C^g as a polynomial in 2^g variables t_ν indexed by $\nu \in \mathbf{F}_2^g$:

$$W_C^g = \sum_{\mathbf{x}^1, \ldots, \mathbf{x}^g \in C} \prod_{i=1}^{n} t_{(\mathrm{wt}(x_i^1), \ldots, \mathrm{wt}(x_i^g))}$$

and similar the *complete g-weight enumerator* cwe_C^g as a polynomial in 4^g variables s_ν where $\nu \in K^g$.

The code C is called *even* if the weights of all codewords are divisible by 2. Note, that a code spanned by an orthogonal system of vectors of even weight is itself even.

The automorphisms of the abelian group K^n which are also isometries for the metric $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$ on K^n form the semidirect product $G = S_3^n{:}S_n$ consisting of the

permutation of the positions together with a permutation of the symbols a, b and c at each position. The *automorphism group* of C is the subgroup of G sending C to itself:

$$\text{Aut}(C) = \{g \in S_3^n : S_n \mid g\,C = C\}.$$

Two codes C and D are called to be equivalent if there is a $g \in G$ with $g\,C = D$. The number of distinct codes equivalent to C is

$$\frac{6^n \cdot n!}{|\text{Aut}(C)|}.$$

Equivalent codes have the same (poly-) weight enumerator, but not necessarily the same complete (poly-) weight enumerator. If C is self-orthogonal, self-dual or even, so it is the equivalent code.

Since K is isomorphic to the additive group of the field $\mathbf{F}_4$, we can interpret every code over K as a code over $\mathbf{F}_4$. Every code linear as $\mathbf{F}_4$-code is linear as Kleinian code, but not conversely. If C is a self-dual Type IV $\mathbf{F}_4$-code for the hermitian scalar product of $\mathbf{F}_4^n$, then it is also a even self-dual Kleinian code (cf. [MOSW78]). Perfect Kleinian codes are the same as perfect $\mathbf{F}_4$-codes, the only perfect Kleinian codes which exist are 1 error correcting codes [Tie73].

Examples of Kleinian codes:

- The $[1, \frac{1}{2}, 1]$-code $\gamma_1 = \{(0), (a)\}$: $|\text{Aut}(\gamma_1)| = 2$, $W_{\gamma_1}(u, v) = u + v$.

- The $[2, 1, 2]$-code $\epsilon_2 = \{(00), (aa), (bb), (cc)\}$: $|\text{Aut}(\epsilon_2)| = 12$, $W_{\epsilon_2}(u, v) = u^2 + 3\,v^2$.

- The $[6, 3, 4]$-Hexacode $\mathcal{C}_6$ spanned by

$$\{(a0a0bb), (a0bba0), (bba0a0), (00aaaa), (aa00aa), (b0b0ca)\}$$

as a Kleinian code. One has $|\text{Aut}(\mathcal{C}_6)| = 2^2 \cdot 2 \cdot 15 \cdot 18 = 2160$, $W_{\mathcal{C}_6}(u, v) = u^6 + 45\,u^2v^4 + 18\,v^6$.

- The Hamming code $\mathcal{H}_m$, $m \geq 2$ of type $[(4^m - 1)/3, (4^m - 1)/3 - m, 3]$ and the extended Hamming code $\overline{\mathcal{H}}_m$, $m \geq 2$ of type $[(4^m - 1)/3 + 1, (4^m - 1)/3 - m, 4]$.

All examples are linear; the first three codes are self-dual; ϵ_2 and $\mathcal{C}_6 \cong \overline{\mathcal{H}}_2$ and $\overline{\mathcal{H}}_m$ are even; besides γ_1, they are equivalent to codes over $\mathbf{F}_4$; the code $\mathcal{H}_m$ is perfect.

Basic results:

The Hamming weight enumerators of C and its dual are related by the following equation.

Theorem 1 (generalized Mac-Williams identity (cf. [Del73]))

$$W_{C^\perp}(u, v) = \frac{1}{|C|} W_C(u + 3v, u - v).$$

Analogues[*]: B: cf. [MS77]; L: cf. [Ser73], Ch. VII, Prop. 16; V: [Zhu90, Höh95].

Proof: For a function f on K^n with values in a ring R we define its transformation $g : K^n \longrightarrow R$ by $g(\mathbf{x}) = \sum_{\mathbf{y} \in K^n} f(\mathbf{y}) \cdot (-1)^{(\mathbf{y}, \mathbf{x})}$. One has the following identity:

$$\frac{1}{|C|} \sum_{\mathbf{x} \in C} g(\mathbf{x}) = \sum_{\mathbf{y} \in C^\perp} f(\mathbf{y}). \tag{1}$$

Proof of (1): $\sum_{\mathbf{x} \in C} g(\mathbf{x}) = \sum_{\mathbf{y} \in K^n} \sum_{\mathbf{x} \in C} f(\mathbf{y})(-1)^{(\mathbf{x}, \mathbf{y})} = |C| \cdot \sum_{\mathbf{y} \in C^\perp} f(\mathbf{y}) + \sum_{\mathbf{y} \notin C^\perp} f(\mathbf{y}) \cdot \sum_{\mathbf{x} \in C} (-1)^{(\mathbf{x}, \mathbf{y})}$. We have to show that the second sum vanishes. To this end, choose for given

$\mathbf{y} \in K^n \setminus C^\perp$ a $\mathbf{x}' \in C$ with $(\mathbf{x}', \mathbf{y}) \neq 0$, i.e., $(-1)^{(\mathbf{x}', \mathbf{y})} = -1$. We get $s = \sum_{\mathbf{x} \in C} (-1)^{(\mathbf{x}, \mathbf{y})} = \sum_{\mathbf{x} \in C} (-1)^{(\mathbf{x}, \mathbf{y}) + (\mathbf{x}', \mathbf{y})} = -s$, which implies $s = 0$ and proves (1).

Now let $f(\mathbf{y}) = u^{n - \mathrm{wt}(\mathbf{y})} v^{\mathrm{wt}(\mathbf{y})}$. We obtain for its transformation

$$
\begin{aligned}
g(\mathbf{x}) &= \sum_{\mathbf{y} \in K^n} f(\mathbf{y}) \cdot (-1)^{(\mathbf{x}, \mathbf{y})} \\
&= \sum_{y_1, \ldots, y_n \in K} u^{n - \mathrm{wt}(y_1) - \cdots - \mathrm{wt}(y_n)} v^{\mathrm{wt}(y_1) + \cdots + \mathrm{wt}(y_n)} (-1)^{x_1 \cdot y_1 + \cdots + x_n \cdot y_n} \\
&= \prod_{i=1}^{n} \left(\sum_{z \in K} u^{1 - \mathrm{wt}(z)} v^{\mathrm{wt}(z)} (-1)^{x_i \cdot z} \right) \\
&= (u + 3v)^{n - \mathrm{wt}(\mathbf{x})} (u - v)^{\mathrm{wt}(\mathbf{x})}.
\end{aligned}
$$

Applying (1) we get for the weight enumerator of $C^\perp$:

$$
W_{C^\perp}(u, v) = \sum_{\mathbf{y} \in C^\perp} f(\mathbf{y}) = \frac{1}{|C|} \sum_{\mathbf{x} \in C} (u + 3v)^{n - \mathrm{wt}(\mathbf{x})} (u - v)^{\mathrm{wt}(\mathbf{x})} = \frac{1}{|C|} W_C(u + 3v, u - v).
$$

$\square$

For the other types of weight enumerators we stay only the results, the proofs are similar.

Theorem 2 (Mac-Williams identity for complete weight enumerators)

$$
\mathrm{cwe}_{C^\perp}(p, q, r, s) = \frac{1}{|C|} \mathrm{cwe}_C(p + q + r + s, \, p + q - r - s, \, p - q + r - s, \, p - q - r + s).
$$

From Theorem 1, we get the following descriptions of the weight enumerators of self-dual codes:

Theorem 3 *Let C be a self-dual $[n, n/2]$-code. Then, the weight enumerator $W_C(u, v)$ is a weighted homogeneous polynomial of weight n in $u + v$ and $v(u - v)$, or equivalently in the weight enumerators of γ_1 and ϵ_2.*

Analogues*: B: [Gle71]; L: cf. [CS93b]; V: [Höh95], Ch. 2.

Proof: From Theorem 1, we see that W_C is invariant under the group $H \cong \mathbf{Z}_2$ generated by the substitution $\frac{1}{2} \left(\begin{smallmatrix} 1 & 3 \\ 1 & -1 \end{smallmatrix} \right)$. The ring of invariants has Molien series $1/\big((1 - \lambda)(1 - \lambda^2)\big)$. (This is the generating function for the multiplicities of the trivial H-representation in the symmetric powers of the defining two dimensional representation of H.) The polynomials $u + v$ and $v(u - v)$ or equivalently W_{γ_1} and W_{ϵ_2} are algebraically independent and generate freely the ring of all invariants. $\square$

Theorem 4 *Let C be an even self-dual $[n, n/2]$-code. Then, the weight enumerator $W_C(u, v)$ is a weighted homogeneous polynomial of weight n in $u^2 + 3v^2$ and $v^2(u^2 - v^2)^2$, or equivalently in the weight enumerators of ϵ_2 and $\mathcal{C}_6$.*

Analogues*: B: [Gle71]; L: cf. [CS93b]; V: see [God89] and [Höh95], Ch. 2.

Proof: This follows from the corresponding result for even self-dual codes over $\mathbf{F}_4$ as proven for example in [MOSW78], Th. 13: The group generated by $S = \frac{1}{2} \left(\begin{smallmatrix} 1 & 3 \\ 1 & -1 \end{smallmatrix} \right)$ and $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right)$ has order 12 and the Molien series of the corresponding ring of invariants is $1/\big((1 - \lambda^2)(1 - \lambda^6)\big)$. $\square$

4

3 Classification of self-dual codes

Let δ_n be the code consisting of all codewords containing only 0's and an even number of a's. This is the even subcode of γ_1^n. One has $\dim(\delta_n) = (n-1)/2$, coset representatives of $\delta_n^\perp/\delta_n$ are given by (0^n), $(a, 0^{n-1})$, (b^n) and (c, b^{n-1}) and its automorphism group consists for $n \geq 2$ of the permutation of the positions together with possible interchanging b and c at every position, i.e., $\mathrm{Aut}(\delta_n) = S_2^n{:}S_n$.

The next theorem describes self-orthogonal codes spanned by vectors of small weight.

Theorem 5 *Minimal weight 1 subcodes of a self-orthogonal code C can be split off: $C \cong D \oplus \gamma_1^l$, with minimal weight of D larger then 1. Self-orthogonal codes generated by weight-2-vectors are equivalent to direct sums of δ_l, $l \geq 2$, and ϵ_2.*

Analogues*: First part: B, L: easy to see; V: cf. [God89], [Höh95], Th. 2.2.8. Second Part: B: [PS75], Th. 6.5; L: cf. [CS93b], Ch. 4; V: Cartan, Killing, [Kac89], [FZ92].

Proof: For the first statement, note that a weight-1-codeword is equivalent to $(0, \ldots, 0, a)$. Then $C = C' \oplus \gamma_1$, where C' is the orthogonal complement in C of the γ_1 spanned by $(0, \ldots, 0, a)$.

For the proof of the second statement, decompose first the code generated by the weight-2-codewords into the direct sum of its indecomposable even components and fix one of them. We have two possibilities:

Case i) There are two weight-2-codewords containing different nonzero entries at the same position.
In this case the component is equivalent to a code containing the two codewords $(aa0\ldots0)$ and $(bb0\ldots0)$. They generate a ϵ_2 subcode and, since ϵ_2 is self-dual, this is the whole component. (The other possible pairs of weight-2-codewords are not orthogonal.)

Case ii) The component is equivalent to a code whose weight-2-codewords have at all positions the value 0 or a.
Inductively, one sees that the component is equivalent to a δ_l, $l \geq 2$. A possible set of generators is given by $(aa0\ldots0)$, $(0aa0\ldots)$, $\ldots$, $(0\ldots0aa)$. $\qquad\square$

Let $\bar{C}$ the subcode of C generated by the weight 1 and 2 codewords. We can describe C by its *gluecode* $\Lambda \subset \bar{C}^\perp/\bar{C}$. The automorphism group of C is given by $\mathrm{Aut}(C) = G_0.G_1.G_2$, where G_0 are the "inner automorphisms" of $\bar{C}$, i.e. those which are fixing the components of $\bar{C}$ and the cosets $\Lambda/\bar{C}$, G_1 are the automorphisms of C fixing the components of $\bar{C}$ modulo G_0 and G_2 is the induced permutation group on the components of $\bar{C}$.

Denote by $M(n)$ resp. $M_e(n)$ the number of distinct (but maybe equivalent) self-dual resp. even self-dual Kleinian codes of length n.

Theorem 6 (Massformula) *The mass constants are given by*

$$M(n) = \prod_{i=1}^{n}(2^i + 1) = \sum_C \frac{6^n \cdot n!}{|\mathrm{Aut}(C)|}$$

where the sum is over equivalence classes of self-dual codes and

$$M_e(n) = \prod_{i=0}^{n-1}(2^i + 1) = \sum_C \frac{6^n \cdot n!}{|\mathrm{Aut}(C)|}$$

where the sum is over equivalence classes of even self-dual codes and n is even.

Analogues: B: cf. [PS75]; L: [Min84]; V: unknown.

Proof: First, we prove the formula for $M(n)$. Let $M(n,k)$ be the number of self-orthogonal codes of dimension k and length n. There are $|(C^\perp \setminus C)/C| = 4^{n-2k} - 1$ different extensions of a self-orthogonal $[n,k]$-code C to a self-orthogonal $[n, k+\frac{1}{2}]$-code $D \supset C$ by choosing one extra vector $x \in C^\perp$. Every self-orthogonal $[n, k+\frac{1}{2}]$-code D arises from $|D\setminus\{0\}| = 4^{k+1/2} - 1$ different codes C. So we get the recursion

$$M(n, k + \frac{1}{2}) = M(n,k) \cdot \frac{4^{n-2k} - 1}{4^{k+1/2} - 1}.$$

Together with $M(n,0) = 1$ we obtain

$$M(n) = M(n, n/2) = \prod_{i=0}^{n-1} \frac{4^{n-i} - 1}{2^{i+1} - 1} = \prod_{i=1}^{n} (2^i + 1).$$

The second expression for $M(n)$ describes the decomposition of all self-dual codes into orbits under the action of $S_3^n{:}S_n$.

To get the mass formula for $M_e(n)$, define in a similar way as before $M_e(n,k)$ as the number of even self-orthogonal codes of dimension k and length n. The dual code $C^\perp$ of a even self-orthogonal $[n,k]$-code C contains $\frac{1}{2}(4^{n-k} + (-2)^n)$ vectors of even weight as one can see from Theorem 1. All vectors in a coset $C^\perp/C$ have the same weight modulo 2. So we get in a similar way as above the recursion

$$M_e(n, k + \frac{1}{2}) = M_e(n,k) \cdot \frac{\frac{1}{2}(4^{n-2k} + 2^{n-2k}) - 1}{4^{k+1/2} - 1}.$$

Starting from $M_e(n,0) = 1$ we obtain

$$M_e(n) = M_e(n, n/2) = \prod_{i=0}^{n-1} \frac{2^{2n-2i-1} + 2^{n-i-1} - 1}{2^{i+1} - 1} = \prod_{i=0}^{n-1} (2^i + 1)$$

and again we can express the total number as a sum over the different equivalence classes of codes. $\qquad\square$

For the weighted sum of the Hamming weight enumerators one has

Theorem 7 (Massformula for Hamming weight enumerators)

$$\sum_C \frac{6^n \cdot n!}{|\text{Aut}(C)|} W_C(u,v) = M(n) \cdot (1 + 2^n)^{-1} \cdot [2^n u^n + (u + 3v)^n]$$

where the sum is over equivalence classes of self-dual codes.

$$\sum_C \frac{6^n \cdot n!}{|\text{Aut}(C)|} W_C(u,v) = M_e(n) \cdot (1 + 2^{n-1})^{-1} \cdot \left[2^{n-1} u^n + \frac{1}{2} \{(u + 3v)^n + (u - 3v)^n\}\right]$$

where the sum is over equivalence classes of even self-dual codes.

Analogues: B: [PS75]; L: [Sie35]; V: unknown.

Proof: Let $\mathbf{x}$ be a nonzero vector (of even weight) of length n. Similar as in the proof of Theorem 6 one gets for the number of (even) self-dual codes containing $\mathbf{x}$ the expression

$$\prod_{i=1}^{n-1} (2^i + 1) \quad \text{or} \quad \prod_{i=0}^{n-2} (2^i + 1) \text{ for even codes.}$$

6

From this and Theorem 6 one obtains the result by summing

$$u^{n-\text{wt}(\mathbf{x})}v^{\text{wt}(\mathbf{x})}$$

over all pairs $(\mathbf{x}, C)$, where C is a (even) self-dual code with $\mathbf{x} \in C$, and expanding the resulting sum in two different ways. □

We remark, that the average Hamming weight enumerator for even self-dual Kleinian codes is the same as for even formal self-dual $\mathbf{F}_4$-codes ([MOSW78], Th. 24) although the mass constants are different.

We call a self-dual code *primitive*, if no γ_1 subcode can be split off. A primitive code C is the first one in the chain C, $C \oplus \gamma_1$, ...

Theorem 8 (Relation between even and odd self-dual codes) *There is a 1 : 1-correspondence between isomorphism classes of pairs (C, δ_k), where C is an even self-dual code of even length n and δ_k a subcode (a defined above) inside C (together with the choice of a class $[x]$ in $\delta_k^\perp/\delta_k$ of minimal weight 1, i.e., if $k = 1$ we must choose $x \in K \setminus \{0\}$) and isomorphism classes of self-dual codes D of length $n - k$.*

The code D is primitive if and only if the subcode δ_k is maximal, i.e. not contained in a δ_{k+1} subcode (with corresponding gluevectors $[x]$).

Analogues: B: [CP80]; L: [CS82b]; V: [Höh95], Ch. 3, and [Höha].

Proof: We describe the map from self-dual codes D of length $n - k$ to even self-dual codes of even length n. Denote by $\delta_k^0 = \delta_k$, δ_k^1, δ_k^2 and δ_k^3 the four cosets of δ_k inside $\delta_k^\perp$ such that $(a0^{k-1}) \in \delta_k^1$.

If D is even, let $C = D \oplus (\delta_k^0 \cup \delta_k^2)$. Otherwise we have the decomposition $D_0^\perp = D_0 \cup D_1 \cup D_2 \cup D_3$ of the orthogonal complement of the even subcode D_0 of $D = D_0 \cup D_1$ into four D_0 cosets. Define

$$C = D_0 \oplus \delta_k^0 \cup D_1 \oplus \delta_k^1 \cup D_2 \oplus \delta_k^2 \cup D_3 \oplus \delta_k^3.$$

Note that for $k = 1$ the three cosets δ_k^1, δ_k^2 and δ_k^3 are all equivalent under $\text{Aut}(\delta_1) = S_3$. It is then easy to check that this map describes the claimed 1 : 1-correspondence. □

We call D a *child* of the parent code C. From Theorem 8, we get the following description of the primitive children of an even self-dual code C of length n: Take a position and choose $x \in \{a, b, c\}$ (up to the action of $\text{Aut}(C)$), this gives a self-dual code D of length $n - 1$.
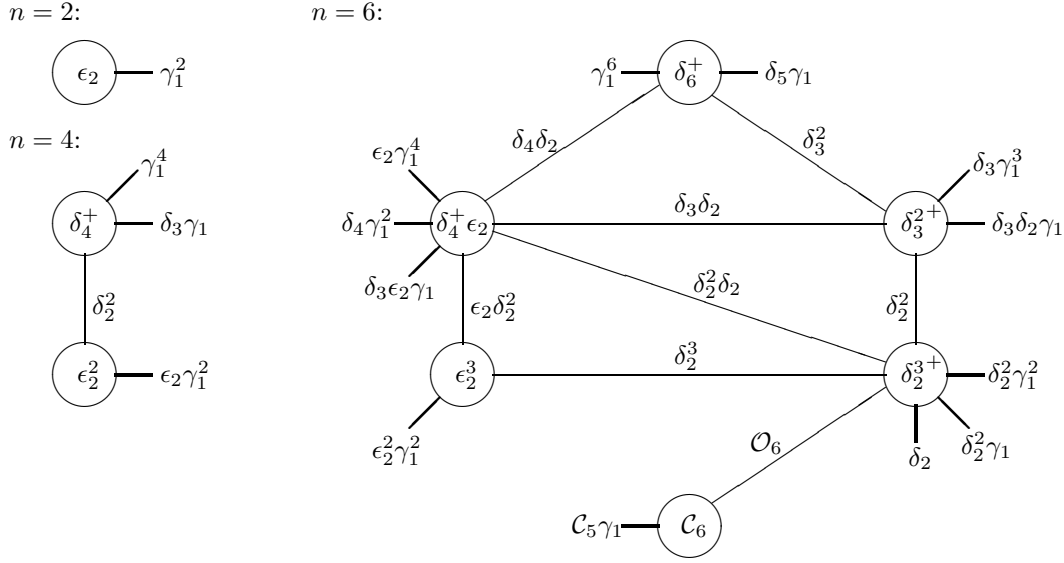
- If the position is not in the support of the subcode $\bar{C}$ generated by the weight-2-codewords, the code D is primitive.

- If the position is in an δ_l, $l \geq 2$, component of $\bar{C}$ we have two cases: If $x \neq a$ then D is again maximal, if $x = a$ the primitive child is obtained by deleting the remaining $l - 1$ positions of δ_l from D.

- If the position is in a ϵ_2 component, the primitive child is obtained by deleting the second position of ϵ_2 from D.

Every non even self-dual code $D = D_0 \cup D_1$ of even length n determines the two *even* self-dual "neighbours" $D_0 \cup D_2$ and $D_0 \cup D_3$, where D_0, D_1, D_2 and D_3 are the four cosets of D_0 in $D_0^\perp$ as above. We define for every even n a "neighbourhood graph" by using the isomorphism classes of even self-dual codes as vertices, the isomorphism classes of non even self-dual codes as edges and "neighbourhood" as incidence relation. An edge corresponding to a non primitive code $D = D' \oplus \gamma_1^l$, $l \geq 1$, is a loop for the vertex corresponding to

Figure 1: The neighbourhood graph for $n = 2$, 4 and 6

$n = 2$:

ϵ_2 — γ_1^2

$n = 4$:

γ_1^4
δ_4^+ — $\delta_3\gamma_1$
δ_2^2
ϵ_2^2 — $\epsilon_2\gamma_1^2$

$n = 6$:

γ_1^6 — δ_6^+ — $\delta_5\gamma_1$
$\delta_4\delta_2$ δ_3^2
$\epsilon_2\gamma_1^4$ $\delta_3\gamma_1^3$
$\delta_4\gamma_1^2$ $\delta_4^+\epsilon_2$ — $\delta_3\delta_2$ — δ_3^{2+} — $\delta_3\delta_2\gamma_1$
$\delta_3\epsilon_2\gamma_1$ $\delta_2^2\delta_2$ δ_2^2
$\epsilon_2\delta_2^2$
ϵ_2^3 — δ_2^3 — δ_2^{3+} — $\delta_2^2\gamma_1^2$
$\epsilon_2^2\gamma_1^2$ $\mathcal{O}_6$ δ_2 $\delta_2^2\gamma_1$
$\mathcal{C}_5\gamma_1$ — $\mathcal{C}_6$

the even code determined from D' through Theorem 8. The edges starting on a vertex C correspond to the orbits of $\mathrm{Aut}(C)$ on the nonzero elements of K^n/C. It is easy to see that the neighbourhood graph is connected for all n. For $n = 2$, 4 and 6 the graph is shown in Figure 1.

Analogues[*]*:* L: [Bor84]; V: not determined.

Theorem 9 *The even self-dual codes up to length* 8 *(together with the subcode* $\bar{C}$, *order of* $G_1.G_2$, *weight enumerator and number of children) are given in Table 1.*

Analogues[*]*:* B: [CP80, CPS92]; L: [Kne57, Nie73]; V: cf. [God89], for $c = 24$ there is a conjectured list in [Sch93].

Proof: Use the list of doubly even self-dual binary codes of length $4n$ [CP80, CPS92] and the construction A described in Section 7 or use Theorem 5 and classify the possibilities for $\bar{C}$ and the gluecodes $\Lambda \subset \bar{C}^\perp/\bar{C}$ directly. $\square$

We checked the result additionally with the mass formula for the Hamming weight enumerator.

Theorem 10 *The non even self-dual codes up to length* 6 *(together with the parent No., the subcode* $\bar{C}$, *order of* $G_1.G_2$ *and the weight enumerator) are given in Table 2.*

Analogues[*]*:* B: [Ple72, PS75]; L: [CS82b, Bor93]; V: [Höh95], Ch. 3, and [Höha].

Proof: Look at the list of even self-dual binary codes of length $4n$ [Ple72, PS75] or apply Theorem 8 to Theorem 9. $\square$

Again we checked the result by the mass formula for the Hamming weight enumerator.

Remark: There is one self-dual code of length 5 without codewords of weight 2: The *shorter Hexacode* $\mathcal{C}_5$. There are two self-dual codes of length 6 without codewords of weight 2: The Hexacode $\mathcal{C}_6$ (even) and the *odd Hexacode* $\mathcal{O}_6$ (non even).

Table 1: Even self-dual codes up to length 8

n	$No.$	$\bar{C}$	$|G_1||G_2|$	A_0	A_2	A_4	A_6	A_8	n_1	n_2
2	1	ϵ_2	1	1	3				1	1
4	1	δ_4	1	1	6	9			2	1
	2	ϵ_2^2	2	1	6	9			1	1
6	1	δ_6	1	1	15	15	33		2	1
	2	$\delta_4\epsilon_2$	1	1	9	27	27		3	2
	3	δ_3^2	2	1	6	33	24		2	1
	4	ϵ_2^3	3!	1	9	27	27		1	1
	5	δ_2^3	3!	1	3	39	21		2	1
	6	$\mathcal{C}_6$	2160	1	0	45	18		1	0
8	1	δ_8	1	1	28	70	28	129	2	1
	2	$\delta_6\epsilon_2$	1	1	18	60	78	99	3	2
	3	$\delta_5\delta_3$	1	1	13	55	103	84	4	2
	4	δ_4^2	2	1	12	54	108	81	2	1
	5	$\delta_4\epsilon_2^2$	2	1	12	54	108	81	3	2
	6	$\delta_4\delta_2^2$	2	1	8	50	128	69	4	2
	7	$\delta_3^2\epsilon_2$	2	1	9	51	123	72	3	2
	8	$\delta_3^2\delta_2$	2	1	7	49	133	66	4	2
	9	$\delta_3\delta_2^2$	2	1	5	47	143	60	7	2
	10	δ_3	120	1	3	45	153	54	3	1
	11	ϵ_2^4	24	1	12	54	108	81	1	1
	12	$\epsilon_2\delta_2^3$	6	1	6	48	138	63	3	2
	13	ϵ_2	2160	1	3	45	153	54	2	1
	14	δ_2^4	24	1	4	46	148	57	2	1
	15	δ_2^4	8	1	4	46	148	57	2	1
	16	δ_2^3	6	1	3	45	153	54	3	1
	17	δ_2^2	16	1	2	44	158	51	4	1
	18	δ_2	48	1	1	43	163	48	4	1
	19	$-$	$6 \cdot 1344$	1	0	42	168	45	1	0
	20	$-$	1152	1	0	42	168	45	1	0
	21	$-$	336	1	0	42	168	45	1	0

Table 2: The non even self-dual codes up to length 6

n	No.	par. No.	$\bar{C}$	$\|G_1\|\|G_2\|$	A_0	A_1	A_2	A_3	A_4	A_5	A_6
1	1	1	γ_1	1	1	1					
2	1	1	γ_1^2	2!	1	2	1				
3	1	1	γ_1^3	3!	1	3	3	1			
	2	2	$\epsilon_2\gamma_1$	1	1	1	3	3			
	3	1	δ_3	1	1	0	3	4			
4	1	1	γ_1^4	4!	1	4	6	4	1		
	2	2	$\epsilon_2\gamma_1^2$	2!	1	2	4	6	3		
	3	3	$\delta_3\gamma_1$	1	1	1	3	7	4		
	4	5	δ_2^2	2!	1	0	2	8	5		
5	1	1	γ_1^5	5!	1	5	10	10	5	1	
	2	2	$\epsilon_2\gamma_1^3$	3!	1	3	6	10	9	3	
	3	3	$\delta_3\gamma_1^2$	2!	1	2	4	10	11	4	
	4	5	$\delta_2^2\gamma_1$	2!	1	1	2	10	13	5	
	5	2	$\delta_4\gamma_1$	1	1	1	6	6	9	9	
	6	4	$\epsilon_2^2\gamma_1$	2!	1	1	6	6	9	9	
	7	1	δ_5	1	1	0	10	0	5	16	
	8	2	$\delta_3\epsilon_2$	1	1	0	6	4	9	12	
	9	3	$\delta_3\delta_2$	1	1	0	4	6	11	10	
	10	5	δ_2^2	2!	1	0	2	8	13	8	
	11	6	$\mathcal{C}_5$	120	1	0	0	10	15	6	
6	1	1	γ_1^6	6!	1	6	15	20	15	6	1
	2	2	$\epsilon_2\gamma_1^4$	4!	1	4	9	16	19	12	3
	3	3	$\delta_3\gamma_1^3$	3!	1	3	6	14	21	15	4
	4	6	$\delta_2^2\gamma_1^2$	$2!^2$	1	2	3	12	23	18	5
	5	4	$\delta_4\gamma_1^2$	2!	1	2	7	12	15	18	9
	6	5	$\epsilon_2^2\gamma_1^2$	$2!^2$	1	2	7	12	15	18	9
	7	3	$\delta_5\gamma_1$	1	1	1	10	10	5	21	16
	8	7	$\delta_3\epsilon_2\gamma_1$	1	1	1	6	10	13	21	12
	9	8	$\delta_3\delta_2\gamma_1$	1	1	1	4	10	17	21	10
	10	9	$\delta_2^2\gamma_1$	2!	1	1	2	10	21	21	8
	11	10	$\mathcal{C}_5\gamma_1$	120	1	1	0	10	25	21	6
	12	6	$\delta_4\delta_2$	1	1	0	7	8	7	24	17
	13	8	δ_3^2	2!	1	0	6	8	9	24	16
	14	9	$\delta_3\delta_2$	1	1	0	4	8	13	24	14
	15	12	$\epsilon_2\delta_2^2$	2!	1	0	5	8	11	24	15
	16	14	δ_2^3	3!	1	0	3	8	15	24	13
	17	15	$\delta_2^2\delta_2$	2	1	0	3	8	15	24	13
	18	16	δ_2^2	2	1	0	2	8	17	24	12
	19	17	δ_2	8	1	0	1	8	19	24	11
	20	18	$\mathcal{O}_6$	$6\cdot 8$	1	0	0	8	21	24	10

Table 3: Number of inequivalent (even) self-dual codes

Type	1	2	3	4	5	6	7	8	9	10	11	12
even	-	1	-	2	-	6	-	21	-		-	≥ 338
odd	1	2	3	6	11	26	59			≥ 392	≥ 12143	

The number of inequivalent (even) self-dual codes of small length n can be read off from Table 3. The number of even codes up to length 8 are obtained from Theorem 9, the number of odd codes up to length 6 from Theorem 10 and 9 and for $n = 7$ it follows from the number of length 7 children of the even length 8 codes. The lower estimates for larger n one obtains from the mass formula.

A complete classification up to $n = 10$ seems possible, but no interesting new structure is expected.

All the self-dual Kleinian codes classified in this section have a nontrivial automorphism group. In analogy to [OP92, Ban88], we expect that this holds only for small length n and that rather almost all self-dual and even self-dual codes have trivial automorphism group. What are the smallest (even) self-dual codes with trivial automorphism groups (cf. [Bac94] for lattices)?

4 Extremal codes

In this section, we study self-dual Kleinian codes of type $[n, n/2, d]$ where d is as large as possible. Let $m = [n/2]$. By Theorem 3 the weight enumerator of a code C can be written as

$$W_C(u, v) = \sum_{i=0}^{m} a_i (u + v)^{n-2i} (v(u - v))^i \tag{2}$$

with unique integral numbers a_i. There is a unique choice of the numbers a_0, ..., a_m such that the right hand side of (2) equals

$$u^n + 0 \cdot u^{n-1}v + \cdots + 0 \cdot u^{n-m}v^m + A_{m+1} u^{n-m-1}v^{m+1} + \cdots + A_n v^n. \tag{3}$$

We call (3) the *extremal weight enumerator* and a code with this weight enumerator *extremal*. So an extremal code has minimal weight $d \geq [n/2] + 1$.

Theorem 11 *The minimal distance d of a self-dual code C of length n satisfies*

$$d \leq \left[\frac{n}{2}\right] + 1.$$

Analogues: B: [MS73]; L: [Sie69]; V: [Höh95], Cor. 5.3.3.

Proof: The proof is parallel to [MS73], Cor. 3. In fact it can be considered as "case 5"[†] of that paper for the parameters $w = 1$, $R = 2$, $S = 1$ and $\alpha = 1$. It follows also from the next theorem. ☐

Let C_0 be the even subcode of C as in the proof of Theorem 8. To study extremal codes in more detail, we need the definition of the *shadow* C' of C: We set $C' = C_0^\perp \setminus C$ if C is not even and $C' = C$ otherwise.

[†] "Case 4" was defined in [MOSW78].

Lemma 1 *If the weight enumerator of C is written as*

$$W_C(u,v) = P_C(W_{\gamma_1}, W_{\epsilon_2}) = Q_C(W_{\gamma_1}, W_{\epsilon_2} - W_{\gamma_1^2})$$

with weighted homogeneous polynomials $P_C(x,y)$ and $Q_C(x,y)$, then for the shadow one has

$$W_{C'}(u,v) = P_C(W_{\gamma_1'}, W_{\epsilon_2}) = Q_C(W_{\gamma_1'}, W_{\epsilon_2} - W_{\gamma_1'^2}).$$

Proof: We show $W_{C'}(u,v) = \frac{1}{|C|}W_C(u+3v, (-1)(u-v))$ from which the lemma follows.

If $C = C'$ is even this is Theorem 1. Otherwise, we get from there

$$
\begin{aligned}
W_{C'}(u,v) &= W_{C_0^\perp}(u,v) - W_C(u,v) = \frac{2}{|C|}W_{C_0}(u+3v, u-v) - W_C(u,v) \\
&= \frac{1}{|C|}\left[W_C(u+3v, u-v) + W_C(u+3v, (-1)(u-v))\right] - W_C(u,v) \\
&= \frac{1}{|C|}W_C(u+3v, (-1)(u-v)). \qquad \square
\end{aligned}
$$

Theorem 12 *There are exactly five extremal codes: γ_1, ϵ_2, δ_3^+, the shorter Hexacode $\mathcal{C}_5$ and the Hexacode $\mathcal{C}_6$.*

Analogues: B: [MS73, War76]; L: [COS78]; V: [Höh95], Th. 5.3.2.

For the corresponding extremal weight enumerators see Table 1 and 2.

Proof: The existence and uniqueness of an extremal code for $n = 1$, 2, 3, 5 and 6 can directly be read off from Table 1 and 2.

The nonexistence for $n = 4$ follows also from this tables, so we must prove the nonexistence for $n > 6$. We can assume C is non even since for an even code we will show (Theorem 15) that for the minimal weight d one has $d \leq 2[n/6] + 2$. But from $d \geq [n/2] + 1$, we get $n = 2$ or 6. Now we are using the shadow C' of C. From Lemma 1, we get for its weight enumerator for $n = 7, 8, \ldots, 11$:

n	7	8	9	10	11
$W_{C'}(u,v)$	$\frac{7}{4}u^6v + \cdots$	$-\frac{13}{8}u^8 + \cdots$	$-\frac{9}{4}u^8v + \cdots$	$\frac{23}{8}u^{10} + \cdots$	$\frac{33}{8}u^{10}v + \cdots$

Since $W_{C'}$ must have non negative integral coefficients, there exists no extremal codes for $7 \leq n \leq 11$. For $n \geq 12$, the coefficient A_{m+2} of $W_C(u,v)$ is always negative. We will sketch the proof:

Let $m = [n/2]$ and replace u by 1. Expanding $(1+v)^{-n}$ in powers of $\phi = \frac{v(1-v)}{(1+v)^2}$ one gets by the Bürmann Lagrange Theorem

$$(1+v)^{-n} = \sum_{k=0}^{m} b_k \phi^k + \sum_{k=m+1}^{\infty} b_k \phi^k \tag{4}$$

with

$$b_k = \frac{1}{k!}\frac{d^{k-1}}{dv^k}\left[\frac{d(1+v)^{-n}}{dv}\left(\frac{v}{\phi}\right)^k\right]\Bigg|_{v=0}.$$

Comparing expansion (4) with (2) and (3) yields $b_k = a_k$ for $k = 0, \ldots, m$. Furthermore, $A_{m+1} = -b_{m+1}$, $A_{m+2} = -b_{m+2} + 3(m+1)b_{m+1} - n$. Now one estimates with the saddle-point method b_{m+1} and b_{m+2} and shows that $A_{m+2} < 0$ for m large enough. The smaller n are checked by a direct computation. $\qquad \square$

Remarks: Similar as in [CS90c, CS90b, CS91] one can refine the bound of Theorem 11 to obtain $d \leq 2[n/5] + O(1)$ by using the shadow code.

For the difference $D_C(u,v) = W_{C_2}(u,v) - W_{C_3}(u,v)$ one has the result

$$D_C(u,v) \in \begin{cases} \mathbf{Q}[W_\epsilon, W_{\mathcal{C}_6}], & \text{if } n \text{ is even,} \\ v(u^2 - v^2)\mathbf{Q}[W_\epsilon, W_{\mathcal{C}_6}], & \text{if } n \text{ is odd.} \end{cases}$$

This result can be used as in [CS90c, CS90b, CS91] to discuss for small n the "weakly" extremal codes meeting the stronger bound for d. As an example, for $n = 5$ we obtain $D_C(u,v) = c \cdot v(u^2 - v^2)(u^2 + 3v^2)$.

Instead of looking for codes with large minimal weight, one can ask the same question for the shadow itself. For self-dual codes with shadows of large minimal weight one gets similar results as recently described by N. Elkies and the author:

Theorem 13 *The minimal weight h of the shadow C' of a self-dual code C of length n satisfies $h \leq n$, with equality if and only if $C \cong \gamma_1^n$.*

Analogues*: B: [Elk95b]; L: [Elk95a]; V: [Höh97], Th. 1.

Proof: Clearly $h \leq n$. By Lemma 1, the weight enumerator of C' is a polynomial $P_C(W_{\gamma_1'}, W_{\epsilon_2})$ in the weight enumerators of γ_1' and ϵ_2, i.e. $W_{C'}(u,v)$ is a homogeneous polynomial of weight n in $2v$ and $u^2 + 3v^2$. So $h = n$ implies $W_{C'}(u,v) = (2v)^n$; but then $W_C(u,v) = (u+v)^n$ and $C \cong \gamma_1^n$. $\qquad\square$

Theorem 14 *Let C be a self-dual code of length n without words of weight 1. Then one has*

i) *C hat at least $(n/2)(5-n)$ codewords of weight 2.*

ii) *The equality holds if and only if $h(C') = n - 2$.*

iii) *In this case the number of codewords of weight $n - 2$ in the shadow is $2^{n-3} \cdot n$.*

Analogues*: B, L: [Elk95b]; V: [Höh97], Th. 2.

Proof: Assume first $h(C') \geq n - 2$. In the same way as in the proof of Theorem 13 we see that $P_C(x,y)$ is a linear combination of x^n and $x^{n-2}y$ and we obtain

$$W_C(u,v) = (u+v)^n - \frac{n}{2}(u+v)^{n-2}\left((u+v)^2 - (u^2 + 3v^2)\right) \tag{5}$$

$$= u^n + 0 \cdot u^{n-1}v + \frac{n}{2}(5-n)u^{n-2}v^2 + \cdots. \tag{6}$$

This proves one direction of ii).

Conversely, we can assume $n < 6$, so the weight enumerator of C can be written as

$$W_C(u,v) = (u+v)^n - \frac{n}{2}(u+v)^{n-2}\left(2uv - 2v^2\right) + \frac{A_2 - (n/2)(5-n)}{4}(u+v)^{n-4}\left(2uv - 2v^2\right)^2.$$

From Lemma 1, we get $A_2 - (n/2)(5-n) \geq 0$ since $W_{C'}(u,v)$ has nonnegative coefficients, and we have i) and the converse of of ii).

Finally, Part iii) follows also from (5) and Lemma 1:

$$
\begin{aligned}
W_{C'}(u,v) &= (2v)^n - \frac{n}{2}(2v)^{n-2}\left((2v)^2 - (u^2 + 3v^2)\right) \\
&= 2^{n-3}n \cdot u^2 v^{n-2} + \left(2^n - n\, 2^{n-3}\right)v^n. \qquad \square
\end{aligned}
$$

There are exactly four such codes meeting the bound $h(C') = n-2$, namely ϵ_2, δ_3^+, $(\delta_2^2)^+$ and $\mathcal{C}_5$.

For even codes there are similar definitions and results. The following result was proven for $\mathbf{F}_4$-codes, but since its proof uses only Theorem 4 it is also true for Kleinian codes.

Theorem 15 (see [MOSW78]) *The minimal distance d of an even self-dual code C of length n satisfies*

$$
d \leq 2\left[\frac{n}{6}\right] + 2.
$$

Analogues: B: [MOS75]; L: [MOS75]; V: [Höh95], Section 5.2.

Remark: The analogous bound for doubly-even binary codes has recently been improved in [KL97, KL00] for large lengths.

An even self-dual code matching this bound is called *extremal*. The corresponding weight enumerator is called the *extremal weight enumerator* of length n. A table of extremal weight enumerators was given in [MOSW78], Table 1.

Again from the $\mathbf{F}_4$ case, the next result follows.

Theorem 16 (see [MOSW78]) *There are no extremal even codes of length $n \geq 136$.*

Analogues: B: [MOS75]; L: [MOS75]; V: no known bound, cf. [Höh95], Section 5.2.

Examples of extremal $\mathbf{F}_4$-codes are known for $n = 2$ (ϵ_2), 4 (ϵ_2^2), 6 ($\mathcal{C}_6$), 8 (3 codes), 10, 14, ..., 22, 28 and 30 (see [CPS79]). They are also examples of extremal even Kleinian codes.

There is no extremal $\mathbf{F}_4$-code of length 12. But there is an extremal even Kleinian code of this length with generator matrix

$$
\begin{pmatrix}
\texttt{aaaaaa} & \texttt{000000} \\
\texttt{bbbbbb} & \texttt{000000} \\
\texttt{000000} & \texttt{aaaaaa} \\
\texttt{000000} & \texttt{bbbbbb} \\
\texttt{a0bab0} & \texttt{aaaa00} \\
\texttt{abccba} & \texttt{bbbb00} \\
\texttt{caca00} & \texttt{a0aaa0} \\
\texttt{cca0a0} & \texttt{b0bbb0} \\
\texttt{ccbaab} & \texttt{a00aaa} \\
\texttt{bccbaa} & \texttt{b00bbb} \\
\texttt{caabcb} & \texttt{aa00aa} \\
\texttt{b0baa0} & \texttt{bb00bb}
\end{pmatrix}
$$

and weight enumerator $W_C(u,v) = u^{12} + 396\, u^6 v^6 + 1485\, u^4 v^8 + 1980\, u^2 v^{10} + 234\, v^{12}$.

Besides the question of the existence of a projective plane of order ten and of a doubly even code of type $[72, 36, 16]$, a $[24, 12, 10]$ self-dual $\mathbf{F}_4$-code was most wanted. After the first

question, also the third question has found a negative answer [LP90]. Since Kleinian codes are combinatorial more natural than $\mathbf{F}_4$-codes, we ask if there is an even self-dual Kleinian code of type $[24, 12, 10]$. This is the smallest open case for extremal even Kleinian codes.

Good even and doubly even self-dual binary codes meeting the Gilbert-Varshamov bound exist, as was shown by using the mass formula for the Hamming weight enumerator [MST72]. A similar result holds for lattices (see [MH73], Ch. II). We expect the same for self-dual and even self-dual Kleinian codes.

5   Constant weight codes and generalized t-designs

Let X_k be the fiber over k of the weight map $\mathrm{wt} : K^n \longrightarrow \{0, 1, \ldots, n\}$. We can write it as the (not two point) homogenous space $X_k = G/H = S_3^n{:}S_n/(S_2^k{:}S_k \times S_3^{n-k}{:}S_{n-k})$. The H-module structure of the function space $L_2(X_k)$ for general alphabets instead of K has been studied in [Dun76]. The space X_k carries the structure of a symmetric association scheme, called the nonbinary Johnson scheme (cf. [TAG85]) as follows: A pair $(\mathbf{x}, \mathbf{y}) \in X_k \times X_k$ belongs to the relation $R_{r,s}$, with r, $s \in \{0, 1, \ldots, k\}$, $r \leq s$, if $r = \#\{i \mid x_i = y_i \neq 0\}$ and $s = \#\{i \mid x_i \neq 0, \ y_i \neq 0\}$. This structures allow one to use the usual association scheme methods to study subsets $Y \subset X_k$ (cf. [DL98]). [‡]

Here, we use the definition of a generalized t-designs as in [Del73]: An element $\mathbf{x} \in K^n$ is said to be covered by an element $\mathbf{y} \in K^n$ if each nonzero component x_i of $\mathbf{x}$ is equal to the corresponding component y_i of $\mathbf{y}$. A *generalized $t-(n, k, \mu)$ design (of type 3)* is a nonempty subset $Y \subset X_k$ such that any element of X_t is covered by exactly μ elements from Y. For $t = 2$, this definition is identical with the notion of a *group divisible incomplete block design* with n groups of 3 elements, blocksize k and $\lambda_1 = 0$, $\lambda_2 = \mu$ introduced in [BN39].

As an example, the three codewords of weight 2 in ϵ_2 form a generalized 1-$(2, 2, 1)$ design. The next result describes a method to obtain generalized 2-designs.

Theorem 17 *Let C be an extremal even code of length $n = 6k$. Then, the codewords of C of fixed non-zero weight form a generalized 2-design.*

Analogues: B: [AM69]; L: [Ven84]; V: unknown.

Proof: This follows from Th. 5.3. in [Del73], a generalization of the Assmus and Mattson theorem: By Theorem 15, there are at most $\frac{1}{2}\big(n - (2(n/6) + 2)\big) + 1 = 2(n/6)$ nonzero weights in such a code. Note, that our scalar product on K defines a required identification map $\chi_{(.)} : K \longrightarrow \mathrm{Hom}(K, \mathbf{C}^*)$. $\qquad\square$

The result applies in particular to the unique extremal even code of length 6, the Hexacode $\mathcal{C}_6$ and the extremal even code of length 12 given in the last section. The generalized 2-$(6, 4, 2)$ and 2-$(6, 6, 2)$ designs formed by the vectors of the Hexacode of weight 4 and 6 are unique.

In this case, the design property can also be obtained from the following result about $\mathrm{Aut}(\mathcal{C}_6)$:

Theorem 18 *The automorphism group of the Hexacode acts transitively on the weight 2 vectors in K^6.*

[‡]I like to thank C. Bachoc for mentioning the references [Dun76, TAG85, DL98, Del73, Bac99] to me.

Table 4: Orbits of $\mathrm{Aut}(\mathcal{C}_6)$ in K^6

weight k	name	Size	Distance to $\mathcal{C}_6$	nearest codeword(s)
0	A_0	1	0	A_0
1	A_1	18	1	A_0
2	A_2	135	2	$A_0, 2 \times A_4$
3	A_3	180	1	A_4
3	B_3	360	2	$3 \times A_4$
4	A_4	45	0	A_4
4	B_4	360	1	A_4
4	C_4	540	2	$3 \times A_4$
4	D_4	270	2	$2 \times A_4, A_6$
5	A_5	270	1	A_4
5	B_5	108	1	A_6
5	C_5	1080	2	$2 \times A_4, A_6$
6	A_6	18	0	A_6
6	B_6	216	1	A_6
6	C_6	45	2	$3 \times A_4$
6	D_6	270	2	$A_4, 2 \times A_6$
6	E_6	180	2	$3 \times A_6$

Analogues: B: [Mat61, Car31]; L: [GS87, HS79]; V: unknown.

Proof: By computing the double cosets $(S_2^k{:}S_k \times S_3^{6-k}{:}S_{6-k}) \backslash S_3^6 / \mathrm{Aut}(\mathcal{C}_6)$ for $k = 0, 1, \ldots, 6$, we get the orbit decomposition of K^6 under $\mathrm{Aut}(\mathcal{C}_6)$ as shown in Table 4. There is only one orbit for $k = 2$. $\qquad\square$

This gives also the information about the structure of the deep holes and the cocode $K^6/\mathcal{C}_6$.

Theorem 19 *The covering radius of the Hexacode $\mathcal{C}_6$ is 2. There is one type of deep holes in K^6. Representatives are the $\mathrm{Aut}(\mathcal{C}_6)$-orbits A_2, B_3, C_4, D_4, C_5, C_6, D_6 and E_6. For every deep hole there are exactly three codewords with distance 2. The three orbits A_0, A_1 and C_6 form a complete system of representatives for the cocode $K^6/\mathcal{C}_6$, representing the cosets of minimal weight 0, 1 and 2, respectively.*

Analogues: B: [CS90d]; L: partially [CPS82, BCQ93, Bor98]; V: unknown.

The 135 deep holes of weight 2 are partioned into 45 sets of "trios", the members of each trio are representing the same coset in $K^6/\mathcal{C}_6$. The subcode of $\mathcal{C}_6$ generated by pairs of members in a trio forms a frame which corresponds to a twisted construction of $\mathcal{C}_6$ from a D_8^*/D_8-code (cf. the end of section 7).

From the next theorem, one deduces immediately that the 18 vectors of weight 6 in the Hexacode are the smallest possible number of elements necessary to form a generalized 2-design with $n = k = 6$.

Theorem 20 (Th. 5 and 6 in [BC52]) *For the number of elements of a generalized 2-(n, k, λ) design Y of type 3 one has*

$$|Y| \geq \begin{cases} 3n, & \text{for } k < n, \\ 2n + 1, & \text{for } k = n. \end{cases}$$

Analogues: B: [RCW75], L: [DGS77], V: unknown.

The set of the 45 weight 4 vectors in the Hexacode has the smallest cardinality for a generalized $2 - (6, 4, \lambda)$ design.

By taking the 253 of the 759 vectors of weight 8 in the binary Golay code having first coordinate 1, one gets the essentially only tight 4-design [Bre79]. The 196560 vectors of squared length 4 in the Leech lattice form the only tight spherical 11-design [BD79, BD80] in dimension greater then 2. This leads to the question: Is there a good notion of tight generalized t-designs, using a bound generalizing Theorem 20 for its definition, characterizing one of the two designs belonging to the Hexacode?

6   Lexicographic codes

The *lexicographic code* of length n and minimal distance d is defined by the greedy algorithm: After writing down the elements of K^n in lexicographic order one chooses in every step the lexicographic first word which has distance at least d to the already chosen codewords.

Theorem 21 (Conway-Sloane [CS86]) *The lexicographic code of length* 2 *and minimal distance* 2 *is* ϵ_2. *The lexicographic code of length* 6 *and minimal distance* 4 *is the Hexacode* $\mathcal{C}_6$.

Analogues: B: [CS86]; L: [CS82a].

Define *self-orthogonal lexicographic codes* by restricting the choice of the next codeword to the dual code of the code spanned by the codewords already chosen. This is some analogy to the definition of integral laminated lattices.

Theorem 22 *The self-orthogonal lexicographic codes with minimal distance* 1, 2, 3 *and* 4 *are "periodic" under direct sum. The periods are* 1, 2, 5 *and* 6 *with periodicity elements* γ_1, ϵ_2, $\mathcal{C}_5$ *and* $\mathcal{C}_6$ *respectively.*

Analogues: B: c_2, H_8, g_{22} and g_{24} [Mon96]; L: $\mathbf{Z}$, E_8, Λ_{23} and Λ_{24} [PP85, CS83]; V: V_{Fermi}, V_{E_8}, $VB^\natural$ and $V^\natural$.

7   Relations to binary codes, lattices and vertex operator algebras

In this section, we assume that the reader is familiar with the notation of a vertex operator algebra (VOA) and a vertex operator super algebra (SVOA) (see [FLM88, FHL93, Kac97] for an introduction). All (S)VOA's are assumed to be simple, unitary and "nice" (cf. [Höh95], Ch. 1).

All the definitions and results of this work have analogies for binary codes, lattices and VOA's, although for VOA's the theory is not completely developed. Analogously to the relation between binary codes and lattices and between lattices and VOA's one has two constructions (an "untwisted" and a "twisted" one) for binary codes from Kleinian codes.

Construction A: Define a map ρ_A from Kleinian codes of length n to binary codes of length $4n$ by

$$\rho_A(C) := \widehat{C} + d_4^n,$$

where $\widehat{} : K^n \longrightarrow \mathbf{F}_2^{4n}$ is the map induced from $\widehat{} : K \cong (D_4^*/D_4) \longrightarrow (D_2^*/D_2)^2 \cong \mathbf{F}_2^4$, $0 \mapsto (0000)$, $a \mapsto (1100)$, $b \mapsto (1010)$, $c \mapsto (0110)$ and $d_4^n = \{(0000), (1111)\}^n$. So every codeword in C is replaced with 2^n binary codewords in $\mathbf{F}_2^{4n}$.

Construction B: Assume n is even. Then

$$\rho_B(C) := \widehat{C} + (d_4^n)_0 \cup \widehat{C} + (d_4^n)_0 + \begin{cases} (1000 \; \ldots \; 1000 \; 1000), & \text{if } n \equiv 0 \pmod 4, \\ (1000 \; \ldots \; 1000 \; 0111), & \text{if } n \equiv 2 \pmod 4, \end{cases}$$

where $\widehat{} : K^n \longrightarrow \mathbf{F}_2^{4n}$ is the map as defined before and $(d_4^n)_0$ is the subcode of d_4^n consisting of vectors of weight divisible by 8.

Lemma 2 *If C is a linear, self-dual resp. even Kleinian code then $\rho_A(C)$ is a linear, even self-dual resp. doubly even binary code. The same is true for $\rho_B(C)$ if the length is even.* $\square$

Lemma 3 *For the weight enumerators one has:*

$$
\begin{aligned}
W_{\rho_A(C)}(x, y) &= W_C(x^4 + y^4, 2x^2y^2), \\
W_{\rho_B(C)}(x, y) &= \frac{1}{2}W_C(x^4 + y^4, 2x^2y^2) + \frac{1}{2}(x^4 - y^4)^n + \\
&\qquad \frac{2^n}{2} \cdot \left((x^3y + xy^3)^n + (-1)^{n/2}(x^3y - xy^3)^n \right).
\end{aligned}
$$
$\square$

Analogues: B–L: see [CS93b], Ch. 7; L–V: cf. [Höh95], Ch. 1 and 5.

Remarks:

$\rho_B(\mathcal{C}_6)$ gives the Golay code. (This is the MOG-construction.)

If we denote the untwisted (twisted) construction from binary codes to lattices and from lattices to VOA's also with ρ_A resp. ρ_B (cf. [DGH98]) then one has

$$\rho_X(\rho_Y(\rho_Z)) = \rho_{\pi(X)}(\rho_{\pi(Y)}(\rho_{\pi(Z)})), \quad \text{with } X, Y, Z \in \{A, B\} \text{ and } \pi \in S_3.$$

Markings and frames:

A *marking* for a code C is the choice of a vector $\mathcal{M} \in (K \setminus \{0\})^n$. Table 4 shows that there exist 5 inequivalent markings for the Hexacode.

For $i = 1, \ldots, n$ we define

$$I_i = \begin{cases} \{(4i-3, 4i-2), (4i-1, 4i)\}, & \text{if } \mathcal{M}_i = a, \\ \{(4i-3, 4i-1), (4i-2, 4i)\}, & \text{if } \mathcal{M}_i = b, \\ \{(4i-3, 4i), (4i-1, 4i-2)\}, & \text{if } \mathcal{M}_i = c. \end{cases}$$

Then $I = \bigcup_{i=1}^n I_i$ is a *marking* for the binary code $\rho_X(C)$ as defined in [DGH98]. As described in [DGH98] one gets from I a D_1-*frame* in $\rho_X(\rho_Y(C))$ (or equivalent a $\mathbf{Z}_4$-code, cf. [CS93a]) and a *Virasoro frame* in $\rho_X(\rho_Y(\rho_Z(C)))$. Since $\text{Aut}(K^n) = S_3:S_n$ acts transitively on $(K \setminus \{0\})^n$ we can assume $\mathcal{M} = (aa \ldots a)$ by replacing C with an equivalent code. For this standard marking we define the *symmetrized (marked) weight enumerator* swe_C as

$$\text{swe}_C(U, V, W) = \text{cwe}_C(U, V, W, W).$$

The *symmetrized marked weight enumerator* of the above marked binary code $\rho_X(C)$ as defined in [DGH98] can be obtained from $\text{swe}_C(U, V, W)$:

Lemma 4

$$\mathrm{smwe}_{\rho_A(C)}(x,y,z) \;=\; \mathrm{swe}_C(x^2+y^2,2xy,2z^2),$$

$$\mathrm{smwe}_{\rho_B(C)}(x,y,z) \;=\; \frac{1}{2}\mathrm{swe}_C(x^2+y^2,2xy,2z^2)+\frac{1}{2}(x^2-y^2)^n +$$
$$\frac{1}{2}\cdot 2^n((x+y)^n+(-1)^{n/2}(x-y)^n)z^n. \qquad\qquad \square$$

Analogues: B–L: [DGH98]; L–V: [DGH98].

We remark that the symmetrized marked weight enumerator of an even self-dual code belongs to a ring of polynomials with Molien series $\left(1+\lambda^4\right)/\left((1-\lambda^2)^2(1-\lambda^6)\right)$ generated by $p_2 = x^2 + 2\,y^2 + z^2$, $q_2 = x^2 + 4\,y\,z - z^2$, $p_4 = x^4 + 8\,y^4 + 6\,x^2\,z^2 + z^4$, $p_6 = x^6 + 6\,x^2\,y^4 + 4\,y^6 + 24\,x^2\,y^3\,z + 12\,x^2\,y^2\,z^2 + 6\,y^4\,z^2 + 8\,y^3\,z^3 + 3\,x^2\,z^4$ subject to one relation for p_4^2.

Now, we describe how codes and lattices can be understood in terms of VOA's. Let V be a rational VOA whose intertwiner algebra is abelian, i.e. the set of irreducible V-modules form an abelian group G under the fusion product (cf. [DL93]). The map $\alpha : G \longrightarrow \mathbf{C}^*$, $M \mapsto e^{2\pi i h(M)}$, where $h(M)$ is the conformal weight of the V-module M defines a quadratic form on G and can be interpreted as an element of $H^4(K(G,2),\mathbf{C}^*)$; where $K(G,2)$ is the Eilenberg-MacLane space with $\pi_2(K(G,2)) \cong G$ (see [Höhb]). Another description is the following: The monodromy structure of the intertwiner operators of V give rise to a three dimensional topological quantum field theory which is example I.1.7.2 of [Tur94].

The fusion algebra of $V^{\otimes n}$ is $\mathcal{F}(V^{\otimes n}) \cong \mathbf{Z}[G^n]$. A subgroup $C \subset G^n$ is called an *even self-orthogonal linear code* if C is an isotropic subspace of the quadratic space (G^n, α^n). It is proven in [Höhb] that (simple) VOA-extensions W of $V^{\otimes n}$ are in one to one correspondence with such codes C; in particular, $W = \bigoplus_{\alpha \in C} M_\alpha$ has a unique VOA-structure up to isomorphism extending the VOA-structure of $V = M_0$. The uniqueness follows from $H^3(K(C,2),\mathbf{C}^*) = 0$. Similar remarks hold for odd self-orthogonal codes and SVOA's.

As an example, let V be the lattice-VOA V_L belonging to an even integral positive definite lattice L of rank n. In this case $G = L^*/L$ with α induced from $e^{2\pi i \frac{(.,.)}{2}} : \mathbf{R}^n \longrightarrow \mathbf{C}^*$, where $(.,.)$ is the standard scalar product of $\mathbf{R}^n$. In fact, the triple (G, α, n) is a complete invariant of the *genus* of L (see [Nik80]).

Since the VOA belonging to the root lattice D_4 of Spin(8) has four irreducible modules with the conformal weights 0 and three times $\frac{1}{2}$ and one has $\mathcal{F}(V_{D_4}) \cong \mathbf{Z}[\mathbf{Z}_4]$, we get from the above example the following description of Kleinian codes:

Even (odd) self-dual K-codes of length n are the same as self-dual VOA's (SVOA's) of rank $4n$ with sub-VOA $V_{D_4}^{\otimes n}$, the n-th tensor product of the VOA associated to the Level-1-representation of the affine Lie algebra $\widehat{\mathrm{Spin}}(8)$. The automorphism group of K^n corresponds to the outer automorphism group of $V_{D_4^{\otimes n}}$ in the VOA-sense (Triality of Spin(8)!); the group algebra $\mathbf{Z}[K^n]$ is the fusion algebra of $V_{D_4^{\otimes n}}$.

One has a similar description for binary codes in terms of the lattice-VOA $V_{A_1}^{\otimes n}$.

For V be the (non rational) Heisenberg-VOA V_h of rank 1 on has $G^n = \mathbf{R}^n$, $\alpha = e^{2\pi i \frac{(.,.)}{2}}$. Isotropic subspaces are even integral lattices, i.e., we have a 1 : 1-correspondence between rank n VOA's containing the Heisenberg-VOA $V_h^{\otimes n} \cong V_{h^n}$ and even integral lattices.

The description of (marked/framed) Kleinian codes, binary codes and lattices in terms of VOA's is summarized in the next table.

Table 5: Extremal odd Codes, Lattices and SVOA's

Rank	$\frac{1}{2}$	1	$\frac{3}{2}$	2	$\frac{5}{2}$	3	$\frac{7}{2}$	4	$\frac{9}{2}$	5	$\frac{11}{2}$	6	$\frac{13}{2}$	7	$\frac{15}{2}$
K-Codes								γ_1							
								$\downarrow$							
$\mathbf{F}_2$-Codes			c_2					c_2^2				c_2^3			
			$\downarrow$					$\downarrow$				$\downarrow$			
Lattices		$\mathbf{Z}$		$\mathbf{Z}^2$		$\mathbf{Z}^3$		$\mathbf{Z}^4$		$\mathbf{Z}^5$		$\mathbf{Z}^6$		$\mathbf{Z}^7$	
		$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$	
SVOA's	V_F	V_F^2	V_F^3	V_F^4	V_F^5	V_F^6	V_F^7	V_F^8	V_F^9	V_F^{10}	V_F^{11}	V_F^{12}	V_F^{13}	V_F^{14}	V_F^{15}

Rank	8	12	14	15	$\frac{31}{2}$	20	22	23	$\frac{47}{2}$	24
K-Codes	ϵ_2	δ_3^+				$\mathcal{C}_5$				$\mathcal{C}_6$
	$\downarrow$	$\downarrow$								
$\mathbf{F}_2$-Codes	e_8	d_{12}^+	$(e_7+e_7)^+$				g_{22}			g_{24}
	$\downarrow$	$\downarrow$	$\downarrow$							
Lattices	E_8	D_{12}^+	$(E_7+E_7)^+$	A_{15}^+				O_{23}		Λ_{24}
	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$						
SVOA's	V_{E_8}	$V_{D_{12}^+}$	$V_{(E_7+E_7)^+}$	$V_{A_{15}^+}$	$V_{E_{8,2}^+}$				$VB^\natural$	$V^\natural$

The arrow $\downarrow$ denotes construction ρ_A and the rank of a Kleinian code of length n is defined as $4n$.

Object	Rank	Sub-VOA (framed)	Group	Sub-VOA	Group
K-codes	$4n$	$V_{D_4,*}^{\otimes n}$	$2^n{:}S_n$	$V_{D_4}^{\otimes n}$	$S_3^n{:}S_n$
binary codes	$2n$	$V_{D_2}^{\otimes n}$	$2^n{:}S_n$	$V_{A_1}^{\otimes 2n}$	S_{2n}
lattices	n	$V_{D_1}^{\otimes n}$	$2^n{:}S_n$	$V_h^{\otimes n}$	$SO(n)$
VOA's	$n/2$	$L_{1/2}(0)^{\otimes n}$	cf. [GH]	Vir_n	"$\mathrm{Aut}(\mathcal{F}(\mathrm{Vir}_n))$"

Construction A (including marking/frames) can now be completely understood in terms of VOA's as indicated in following table of inclusions:

$$
\begin{array}{ccc|ccc|ccc}
\multicolumn{3}{c|}{\text{K--B}} & \multicolumn{3}{c|}{\text{B--L}} & \multicolumn{3}{c}{\text{L--V}} \\
\hline
V_{D_4,*}^{\otimes n} & \supset & V_{D_2}^{\otimes 2n} & V_{D_2}^{\otimes n} & \supset & V_{D_1}^{\otimes 2n} & V_{D_1}^{\otimes n} & \supset & L_{1/2}(0)^{\otimes 2n} \\
\cup & & \cup & \cup & & \cup & \cup & & \cup \\
V_{D_4}^{\otimes n} & \supset & V_{A_1}^{\otimes 2n} & V_{A_1}^{\otimes 2n} & \supset & V_h^{\otimes 2n} & V_h^{\otimes n} & \supset & \mathrm{Vir}_n
\end{array}
$$

For all four theories one has analogous basic objects. We display their relations in Table 5.

Final Remarks: The way from Kleinian codes over binary codes and lattices to VOA's is not canonically given. There is no way to see what is the next step. But in the other direction there is in some sense always a canonical choice: Consider the self-dual objects of rank 24. There are always two objects without "roots": An even and an odd one.[§] Look at the even subobject of the odd one. Exactly one of its 4 modules contains "roots". Take the direct sum of the even subobject and the "root"-module and consider inside the subobject

---

[§] In the case of vertex operator algebras the uniqueness of the moonshine module $V^\natural$ and the odd moonshine module $VO^\natural$ is only a conjecture.

generated by the "roots". It is a direct product of indecomposable objects. The next step is now represented by "Codes" over the modules of one such indecomposable object.

There is one more such step before Kleinian codes, namely codes over the 3-dimensional topological quantum field theory belonging the vertex operator algebra V_{D_8}.

Some historical comments and further developments:

I found the structure of Kleinian codes as developed in this paper by searching for an analogue of the shorter Moonshine module in autumn 1995. This was motivated by the work on Virasoro frames inside the Moonshine module. The weight enumerator of the shorter Hexacode (which is not a $\mathbf{F}_4$-code) dropped out. Compare the last paragraphs above.

A first outline of this paper was distributed during the first two month of 1996 including all the results but most proofs not yet written up in Kleinian code language. Some other preliminary versions, but now without Section 5, were distributed in summer 1996. The only exception to this is the extremal code of length 12. I tried to find such a code by hand (cf. letter to Hirzebruch [Höh96]), but without success. Back in Germany in October 1996, it popped up on the screen of my old AT-286 PC after a few minutes (or hours) by running a simple back-tracking algorithm. This code was also found in [CRSS98], where the authors applied the theory of Kleinian codes to quantum codes. This paper became the stimulus of a lot of research on quantum codes. It seems that only a late 1996 preprint found the widest distribution. I am sorry about the delay in publishing the paper. I like to thank C. Bachoc, J.-L. Kim and V. Pless for comments on the final version.

Since that time, Kleinian codes have been investigated further. In the following, I will give an overview.

Section 2: The invariant ring for the complete weight enumerator of even self-dual Kleinian codes has been given in [RS98a].

Section 3: Examples of cyclic self-dual codes for all odd length have been given by M. Ran and J. Snyders in [RS00].

It was pointed out to me by J.-L. Kim that the papers [GHKPa, BG] are answering partially my question for the smallest codes with trivial automorphism group: There is at least one such code of length 12 (called QC_12g in [GHKPa]; non even) and there are at least 273 such extremal even codes of length 14 (see [BG]). Since all the even codes of length 8 and 10 without weight 2 vectors are extremal, it follows from Section 3 and [BG] that the answer for even self-dual codes must be 12 or 14.

Section 4: The upper bound of Theorem 11 has been sharpened by E. Rains in [Rai98] to $d \leq 2[n/6] + 2 + e$ with $e = 1$ for $n \equiv 5 \pmod 6$ and $e = 0$ else. For $6|n$, a code meeting this bound is even. An analogue sharpened bound for binary codes can also be found in [Rai98] and for odd lattices in [RS98b].

In [GHKPb, GHKPa], Gaborit, Huffman, Kim and Pless classified self-dual Kleinian codes with minimal weight reaching the above bound for length 8, 9 and 11 (there are 5, 8 resp. 1 such codes). They also proved the uniqueness of the extremal even code of length 12. There is no such code for length 13 (see [RS98a]). For even codes, the length 10 has been settled in [BG] (19 codes), where also partial results for length 14 and 18 are obtained.

Section 5: C. Bachoc (see [Bac]) has proven Theorem 17 and some extensions of it for all n by using discrete harmonic analysis on X_k. Interestingly, this approach works only for alphabets with

2, 3 and 4 elements and a unique choice of group structure and bilinear form. For four elements, one gets our scalar product on K. The binary analogue was studied before in [Bac99]. This approach forms the direct analogue to the approach of B. Venkov for lattices [Ven84].

References

[AM69]   E. F. Assmus and H. F. Mattson, *New 5-designs*, J. Combinatorial Theory **6** (1969), 122–151.

[Bac]   Christine Bachoc, *Harmonic weight enumerators of nonbinary codes and MacWilliams identities*, preprint, 1999.

[Bac94]   Roland Bacher, *Unimodular lattices without nontrivial automorphisms*, Internat. Math. Res. Notices (1994), no. 2, 91–95.

[Bac99]   Christine Bachoc, *On harmonic weight enumerators of binary codes*, Designs, Codes and Cryptogr. **18** (1999), 11–28.

[Ban88]   E. Bannai, *Positive definite unimodular lattices with trivial automorphism groups*, Ph.D. thesis, Ohio State Univ., 1988.

[BC52]   R. C. Bose and W. S. Connor, *Combinatorial Properties of Group Divisible Incomplete Block Designs*, Ann. Math. Statistics **23** (1952), 367–383.

[BCQ93]   R. E. Borcherds, J. H. Conway, and L. Queen, *The Cellular Structure of the Leech Lattice*, [CS93b], Chapter 25, pp. 515–523.

[BD79]   E. Bannai and R. M. Damerell, *Tight spherical designs. I*, Journal of the Mathematical Society of Japan **31** (1979), 199–207.

[BD80]   E. Bannai and R. M. Damerell, *Tight spherical designs. II*, J. London Mathematical Soc. (2) **21** (1980), 13–30.

[BG]   Christine Bachoc and Philippe Gaborit, *On Extremal Additive* GF(4) *codes of Length* 10 *to* 18, preprint, 2000.

[BN39]   R. C. Bose and K. R. Nair, *Partially balanced incomplete block designs*, Sankhyā **4** (1939), 337–372.

[Bor84]   R. E. Borcherds, *The Leech lattice and other lattices*, Ph.D. thesis, Cambridge University, 1984.

[Bor93]   R. E. Borcherds, *The* 24-*dimensional odd unimodular lattices*, [CS93b], (see also [Bor84]), pp. 421–426.

[Bor98]   R. E. Borcherds, *Automorphic forms with singularities on Grassmannians*, Invent. Math. **132** (1998), 491–562.

[Bre79]   Andrew Bremner, *A Diophantine equation arising from tight* 4-*designs*, Osaka Journal Math. **16** (1979), 353–356.

[Car31]   R. D. Carmichael, *Tactical configurations of rank two*, Amer. J. Math. **53** (1931), 217–240.

[COS78]   J. H. Conway, A. M. Odlyzko, and N. J. A. Sloane, *Extremal self-dual lattices exist only in dimensions* 1 *to* 8*,* 12*,* 14*,* 15*,* 23 *and* 24, Mathematika **25** (1978), 36–43, see Chapter 19 in [CS93b].

[CP80]   J. H. Conway and V. Pless, *On the Enumeration of Self-Dual Codes*, Journal of Combinatoial Theory, Ser. A **28** (1980), 26–53.

[CPS79]   J. H. Conway, V. Pless, and N. J. A. Sloane, *Self-dual codes over* GF(3) *and* GF(4) *of length not exceeding* 16, IEEE Transactions on Information Theory **25** (1979), 312–322.

[CPS82]   J. H. Conway, R. A. Parker, and N. J. A. Sloane, *The Covering Radius of the Leech Lattice*, Proc. of the Royal Soc. **A380** (1982), 261–290, see Chapter 23 in [CS93b].

[CPS92]   J. H. Conway, V. Pless, and N. J. A. Sloane, *The Binary Self-Dual Codes of Length up to* 32*: A Revised Enumeration*, Journal of Combinatorial Theory, Ser. A **60** (1992), 183–195.

[CRSS98]   A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction via codes over* GF(4), IEEE Trans. Inform. Theory **44** (1998), 1369–1387.

[CS82a]   J. H. Conway and N. J. A. Sloane, *Laminated lattices*, Annals of Mathematics **116** (1982), 593–620, see Chapter 6 in [CS93b].

[CS82b]   J. H. Conway and N. J. A. Sloane, *The unimodular lattices of dimension up to 23 and the Minkowski-Siegel mass constants*, European Journal of Combinatorics **3** (1982), 219–231, see Chapter 16 in [CS93b].

[CS83]   J. H. Conway and N. J. A. Sloane, *Complex and integral laminated lattices*, Transactions of the AMS **280** (1983), 463–490.

[CS86]   J. H. Conway and N. J. A. Sloane, *Lexicographic codes: error correcting codes from game theory*, IEEE Transactions on Information Theory **32** (1986), 337–348.

[CS90a]   Y. Cheng and N. J. A. Sloane, *The Automorphism group of an* [18, 9, 8] *quaternary code*, Discrete Mathematics **83** (1990), 205–212.

[CS90b]   J. H. Conway and N. J. A. Sloane, *A New Upper Bound for the Minimum of an Integral Lattice of Determinant* 1, Bulletin of the American Mathematical Society (New Series) **23** (1990), 383–387.

[CS90c]   J. H. Conway and N. J. A. Sloane, *A New Upper bound on the Minimal Distance of Self-Dual Codes*, IEEE Transactions on Information Theory **36** (1990), 1319–1333.

[CS90d]   J. H. Conway and N. J. A. Sloane, *Orbit and Coset Analysis of the Golay and Related Codes*, IEEE Transactions on Information Theory **35** (1990), 1038–1050.

[CS91]   J. H. Conway and N. J. A. Sloane, *Erratum: A New Upper Bound for the Minimum of an Integral Lattice of Determinant* 1, Bulletin of the American Mathematical Society (New Series) **24** (1991), 479.

[CS93a]   J. H. Conway and N. J. A. Sloane, *Self-dual codes over the Integers Modulo* 4, Journal of Combinatorial Theory, Ser. A **62** (1993), 30–45.

[CS93b]   J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, second ed., Grundlehren der Mathematischen Wissenschaften Band 290, Springer-Verlag, New York, 1993.

[Del73]   Phillippe Delsarte, *Four Fundamental Parameters of a Code and Their Combinatorial Significance*, Information and Control **23** (1973), 407–438.

[DGH98]   Chonying Dong, Robert Griess, and Gerald Höhn, *Framed Vertex Operator Algebras, Codes and the Moonshine Module*, Comm. Math. Phys. **193** (1998), 407–448.

[DGS77]   P. Delsarte, J.-M. Goethals, and J. J. Seidel, *Spherical codes and designs*, Geometriae Dedicata **6** (1977), 363–388.

[DL93]   Chongying Dong and James Lepowsky, *Generalized Vertex Algebras and Relative Vertex Operators*, Progress in Mathematics, Birkhäuser, Boston, 1993.

[DL98]   Phillippe Delsarte and Vladimir I. Levenshtein, *Association schemes and coding theory*, IEEE Transactions on Information Theory **44** (1998), 2477–2504.

[Dun76]   Charles F. Dunkel, *A Krawtchouk Polynomial Addition Theorem and Wreath Products of Symmetric Groups*, Indiana University Mathematics Journal **25** (1976), 335–358.

[Elk95a]   Noam D. Elkies, *A characterization of the $\mathbf{Z}^n$ lattice*, Math. Research Letters **2** (1995), 321–326.

[Elk95b]   Noam D. Elkies, *Lattices and codes with long shadows*, Math. Research Letters **2** (1995), 643–651.

[FHL93]   Igor B. Frenkel, Yi-Zhi Huang, and James Lepowsky, *On Axiomatic Approaches to Vertex Operator Algebras and Modules*, Memoirs of the AMS, Band 104, Nr. 494, American Mathmeatical Society, Providence, 1993.

[FLM88]   Igor Frenkel, James Lepowsky, and Arne Meuerman, *Vertex Operator Algebras and the Monster*, Academic Press, San Diego, 1988.

[FZ92]   Igor B. Frenkel and Yongchang Zhu, *Vertex Operator Algebras associated to Representations of Affine and Virasoro Algebras*, Duke Mathematical Journal **66** (1992), 123–168.

[GH]   Robert Griess and Gerald Höhn, *Virasoro Frames and their Stabilizers for the E_8 Lattice type Vertex Operator Algebra*, preprint, 2000.

[GHKPa]   P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, *On Additive Codes over* GF(4), preprint, 2000.

[GHKPb]   P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, *On the Classification of Extremal Additive Codes over* GF(4), Proceedings of the 37th Allerton conference on communication, control and computing, UIUC, Sep. 1999, pp. 535–544.

[Gle71]   A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3, Gauthier-Villars, Paris, 1971, pp. 211–215.

[God89]   Peter Goddard, *Meromorphic Conformal Field Theory*, In Kac [Kac89], pp. 556–587.

[GS87]   J.-M. Goethals and J. J. Seidel, *Spherical Designs*, Am. Math. Soc., Providence, 1987, pp. 255–272.

[Höha]   Gerald Höhn, *Classification of self-dual Vertex Operator Super Algebras with Rank smaller than* 24, in preparation.

[Höhb]   Gerald Höhn, *Simple current extensions of Vertex Operator Algebras and the Cohomology of $K(\pi, 2)$*, in preparation.

[Höh95]   Gerald Höhn, *Selbstduale Vertexoperatorsuperalgebren und das Babymonster*, Ph.D. thesis, Universität Bonn, 1995, see: Bonner Mathematische Schriften **286**.

[Höh96]   Gerald Höhn, *Letter to Prof. F. Hirzebruch*, 1996.

[Höh97]   Gerald Höhn, *Self-dual Vertex Operator Superalgebras with Shadows of large minimal weight*, Internat. Math. Res. Notices **13** (1997), 613–621.

[HS79]   W. C. Huffman and N. J. A. Sloane, *Most primitive groups have messy invariants*, Advances in Math. **32** (1979), 118–127.

[Huf90]   W. Cary Huffman, *On Extremal Self-dual Quaternary Codes of Lengths 18 to 28, I*, IEEE Transactions on Information Theory **36** (1990), 651–660.

[Huf91]   W. Cary Huffman, *On Extremal Self-dual Quaternary Codes of Lengths 18 to 28, II*, IEEE Transactions on Information Theory **37** (1991), 1206–1216.

[Kac89]   V. G. Kac (ed.), *Infinite Dimensional Lie Algebras and Lie Groups: Proceedings of the Conference Held at CIRM, Luminy, 1988*, Adv. Ser. Math. Phys. **7**, World Scientific, Singapore, 1989.

[Kac97]   Victor Kac, *Vertex algebras for beginners*, University Lecture Series, vol. 10, American Mathematical Society, Providence, RI, 1997.

[KL97]   Ilia Krasikov and Simon Litsyn, *Linear programming bounds for doubly-even self-dual codes*, IEEE Trans. Inform. Theory **43** (1997), 1238–1244.

[KL00]   Ilia Krasikov and Simon Litsyn, *An improved upper bound on the minimum distance of doubly-even self-dual codes*, IEEE Trans. Inform. Theory **46** (2000), 274–278.

[Kne57]   Martin Kneser, *Klassenzahlen definiter quadratische Formen*, Archiv der Mathematik **8** (1957), 241–250.

[LP90]   C. W. H. Lam and V. Pless, *There is no* $(24, 12, 10)$ *self-dual quaternary code*, IEEE Transactions on Information Theory **36** (1990), 1153–1156.

[Mat61]   Émile Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, J. de Math. Pures et. Appl. (Ser. 2) **6** (1861), 241–323.

[MH73]   J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Ergebnisse der Mathematik und ihrer Grenzgebiete Band 73, Springer-Verlag, Berlin, Heidelberg, New York, 1973.

[Min84]   H. Minkowski, *Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten*, Mém. près. par divers savants á l'Acadèmie des Sci. Inst. nat. de France **29** (1884).

[Mon96]   Laura Monroe, *Self-orthogonal greedy codes*, Des. Codes Cryptogr. **9** (1996), 79–83, Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

[MOS75]   C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, *Upper Bounds for Modular Forms, Lattices, and Codes*, Journal of Algebra **36** (1975), 68–76.

[MOSW78]   F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward, *Self-Dual Codes of GF*(4), Journal of Combinatorial Theory, Ser. A **25** (1978), 288–318.

[MS73]   C. L. Mallows and N. J. A. Sloane, *An upper bound for self-dual codes*, Information and Control **22** (1973), 188–200.

[MS77]   F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier Science publishers B.V., Amsterdam, 1977.

[MST72]   F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, *Good self dual Codes exist*, Discrete Mathematics **3** (1972), 153–162.

[Nie73]   H.-V. Niemeier, *Definite quadratische Formen der Dimension* 24 *und Diskriminante* 1, Journal of Number Theory **5** (1973), 142–178.

[Nik80]   V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR Izvestija **14** (1980), 103–167.

[OP92]   Haluk Oral and Kevin T. Phelps, *Almost All Self-dual Codes are Rigid*, Journal of Combinatorial Theory, Ser. A **60** (1992), 264–276.

[Ple72]   V. Pless, *A Classification of self-orthogonal Codes over GF*(2), Discrete Mathematics **3** (1972), 209–246.

[PP85]   W. Plesken and M. Pohst, *Constructing Integral Lattices with prescribed Minimum. I*, Mathematics of Computation **45** (1985), 209–221.

[PS75]   V. Pless and N. J. A. Sloane, *On the Classification and Enumeration of Self-Dual Codes*, Journal of Combinatorial Theory, Ser. A **18** (1975), 313–335.

[Rai98]   E. M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory **44** (1998), 134–139.

[RCW75]   Dijen K. Ray-Chaudhuri and Richard M. Wilson, *On t-designs*, Osaka Journal of Mathematics **12** (1975), 747–744.

[RS98a]   E. M. Rains and N. J. A. Sloane, *Self-dual codes*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 177–294.

[RS98b]   E. M. Rains and N. J. A. Sloane, *The shadow theory of modular and unimodular lattices*, Journal of Number Theory **73** (1998), 359–389.

[RS00]   Moshe Ran and Jkov Snyders, *On Cyclic Reversible Self-Dual Additive Codes with Odd length over* $\mathbf{Z}_2^2$, IEEE Trans. Inform. Theory **46** (2000), 1056–1059.

[Sch93]   A. N. Schellekens, *Meromorphic c = 24 Conformal Field Theories*, Comm. Math. Phys. **153** (1993), 159–185.

[Ser73]   Jean-Pierre Serre, *A course in Arithmetic*, Graduate texts in mathematics, 7, Springer-Verlag, New York, Heidelberg, Berlin, 1973.

[Sie35]   C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Annals of Mathematics **36** (1935), 527–606.

[Sie69]   C. L. Siegel, *Berechnung von Zetafunktionen an ganzzahligen Stellen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1969), no. 10, 87–102.

[Slo78]   N. J. A. Sloane, *Codes over* GF(4) *and Complex Lattices*, Journal of Algebra **52** (1978), 168–181.

[Slo79]   N. J. A. Sloane, *Self-dual codes and lattices*, Relations between combinatorics and other parts of mathematics (Proc. Sympos. Pure Math., Ohio State Univ., Columbus, Ohio, 1978), Proc. Sympos. Pure Math., XXXIV, Amer. Math. Soc., Providence, R.I., 1979, pp. 273–308.

[TAG85]   Hannu Tarnanen, Matti J. Aaltonen, and Jean-Marie Goethals, *On the Nonbinary Johnson Scheme*, Europ. Journal of Combinatorics **6** (1985), 279–285.

[Tie73]   A. Tietäváinen, *On the nonexistence of perfect codes over finite fields*, SIAM Journ. Appl. Math. **24** (1973), 88–96.

[Tur94]   V. G. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, de Gruyter Studies in Mathematics, Walter de Gruyter, Berlin, New York, 1994.

[Ven84]   Boris B. Venkov, *Even unimodular extremal lattices*, Trudy Mat. Inst. Steklov **165** (1984), 43–48.

[War76]   Harold N. Ward, *A Restriction on the Weight Enumerator of a Self-Dual Code*, Journal of Combinatorial Theory, Ser. A **21** (1976), 253–255.

[Zhu90]   Yongchang Zhu, *Vertex Operator Algebras, Elliptic Functions, and Modular Forms*, Ph.D. thesis, Yale University, 1990, appeared as: *Modular invariance of characters of vertex operator algebras,* J. Amer. Math. Soc **9** (1996).